[PDA/cell search warrant 11.2011]
SLT:TRP
F.# 2012R00340

12 M 681

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - - - -X

IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:

THE PREMISES KNOWN AND DESCRIBED AS A SAMSUNG METRO PCS CELLULAR TELEPHONE, BEARING HEX NUMBER A000002A8F0298

THE PREMISES KNOWN AND DESCRIBED AS A SAMSUNG BOOST MOBILE CELLULAR TELEPHONE, BEARING HEX NUMBER A000002A7A0CC6

THE PREMISES KNOWN AND DESCRIBED AS A LG VERIZON CELLULAR TELEPHONE, BEARING SERIAL NUMBER 108CYKJ0054941

THE PREMISES KNOWN AND DESCRIBED AS A SAMSUNG AT&T CELLULAR TELEPHONE, BEARING SERIAL NUMBER RQ6BC00349T

- - - - - - - - - - - - - - - - - - -X

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

EASTERN DISTRICT OF NEW YORK, SS:

JOSEPH A. BARBATO, being duly sworn, deposes and states that he is an Investigator with the Drug Enforcement Administration, duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is located in THE PREMISES KNOWN AND DESCRIBED AS A SAMSUNG METRO PCS CELLULAR TELEPHONE, BEARING HEX NUMBER A000002A8F0298 ("DEVICE 1"); THE PREMISES KNOWN AND DESCRIBED AS

A SAMSUNG AT&T CELLULAR TELEPHONE, BEARING SERIAL NUMBER RQ6BC00349T ("DEVICE 2"); THE PREMISES KNOWN AND DESCRIBED AS A SAMSUNG BOOST MOBILE CELLULAR TELEPHONE, BEARING HEX NUMBER A000002A7A0CC6 ("DEVICE 3"); and THE PREMISES KNOWN AND DESCRIBED AS A LG VERIZON CELLULAR TELEPHONE, BEARING SERIAL NUMBER 108CYKJ0054941 ("DEVICE 4")(collectively, the "SUBJECT DEVICES"), further described in Attachment A, the items described in Attachment B, which constitute evidence, fruits and instrumentalities of a conspiracy to distribute and possess with the intent to distribute narcotics, in violation of Title 21, United States Code, Sections 841 and 846.

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I am an Investigator with the Drug Enforcement Administration ("DEA"). I have been employed by the DEA for 22 years. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for distributing narcotics and the diversion of legally manufactured controlled substances into the illicit market. These investigations are conducted both in an undercover and overt capacity. I have participated in investigations

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

involving search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, (c) information obtained from confidential sources of information, (d) interviews with witnesses and victims, and (e) review of surveillance videos and other records and reports.

3. The DEA is investigating the unlawful conspiracy to distribute and possess with the intent to distribute oxycodone.

I. BACKGROUND

4. In or about the fall of 2011, DEA began an investigation into the diversion of oxycodone and other controlled substances by Frank Farella ("FARELLA"), Steward Mitchell, also known as "Mitchell Steward," ("MITCHELL"), Edward Warren ("WARREN"), Frank Vincent ("VINCENT") and others. The investigation revealed that these individuals illegally obtained oxycodone by doctor-shopping, i.e. visiting several doctors during overlapping periods; and by creating and printing forged

prescriptions for oxycodone which were subsequently filled at various pharmacies in Brooklyn, Queens and Staten Island. DEA obtained records from the New York State Department of Health's Bureau of Narcotic Enforcement ("BNE"), which is responsible for maintaining records of all controlled substance prescriptions filled at pharmacies in New York State. Using the BNE data and the prescriptions obtained from various pharmacies, between August 2009 and February 2012, FARELLA, MITCHELL, WARREN and VINCENT obtained over 40,000 tablets of oxycodone.

b. As a result of the BNE data, I and other DEA agents interviewed doctors listed on the oxycodone prescriptions. With few exceptions, the doctors advised agents that they had not issued the prescriptions and that neither FARELLA, MITCHELL, WARREN nor VINCENT were ever a patient of theirs.

c. I and other agents have conducted surveillance of FARELLA, WARREN AND VINCENT on several dates, and have observed FARELLA and others, including WARREN and VINCENT, travel together to pharmacies to have prescriptions filled. Based on surveillance and other investigation by the DEA, agents also learned that FARELLA, VINCENT and other co-conspirators, including Anthony Cabrera ("CABRERA") and Rosemarie Pecorino ("PECORINO"), were using hotel rooms at the Lyghthouse Inn, located in Brooklyn, New York. Agents observed FARELLA, CABRERA, VINCENT and PECORINO at the Lyghthouse Inn.

d. The investigation has further revealed that on November 3, 2011, FARELLA, MITCHELL and WARREN were arrested by police officers with the New York City Police Department after the officers recovered oxycodone pills and untaxed cigarettes inside of the car in which they were driving. A review of CABRERA's criminal record revealed that in November 2011, CABRERA was arrested by police officers with the New York City Police Department for possession of over 100 blank prescriptions and for possession of a controlled substance.

e. On or about March 2, 2012, DEA agents obtained and executed a search warrant issued on March 2, 2012 by the Honorable Roanne L. Mann in the United States District Court for the Eastern District of New York, for Rooms 132, 148 and 208 at the Lyghthouse Inn. After a search of the hotel rooms, agents recovered from inside the hotel rooms DEVICE 1, DEVICE 2, DEVICE 3, over 100 prescriptions (both blank and filled out in various names), approximately 20 identification cards (including drivers' licenses and Medicaid Benefit cards) in various names, two computers, a printer, prescription receipts from various pharmacies and other items. Agents subsequently arrested FARELLA, WARREN, VINCENT, MITCHELL, CABRERA AND PECORINO.

f. On March 27, 2012, a grand jury sitting in the United States District Court for the Eastern District of New York returned an indictment charging FARELLA, WARREN, VINCENT,

MITCHELL, CABRERA and PECORINO with a conspiracy to possess with intent to distribute oxycodone, in violation of Title 21 U.S.C. § 846, and other related charges.

II. TECHNICAL TERMS

5. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and

downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global

Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer

software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

e. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term-IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices

communicating with each other are in the same state.

g. Electronic mail: Electronic mail, commonly called email or e-mail, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If a sender or recipient of the message does not delete the message, the message can remain on the device indefinitely. If an email user writes a draft message but does not send it, that message may also be saved on the device but may not include all of these categories of data. The SUBJECT DEVICES can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails on the device, and attachments to emails, including pictures and files.

h. Text Messages: Text messaging, or texting, refers to the exchange of brief written text messages between fixed-line phone or mobile phone and fixed or portable

devices over a network, and included messages which contain image, video, and sound content.

i. Facebook/MySpace: Facebook and MySpace are a social networking services and websites. Users of these sites may create a personal profile, add other users as friends, and exchange messages, including automatic notifications when they update their profile. Users must register before using the site. Users can create profiles with photos, lists of personal interests, contact information, and other personal information. Users can communicate with friends and other users through private or public messages and a chat feature. Users can access and store personal information, such as contacts, telephone numbers, and photographs on their accounts.

6. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications, I know that the SUBJECT DEVICES have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA, and are capable of using Facebook/MySpace and other similar programs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the SUBJECT

DEVICES.

III. THE SUBJECT DEVICES

7. As part of this investigation, agents received information from a cooperating witness ("CW") whose information has been corroborated by other evidence in this case, that FARELLA and others recruited several individuals who would allow FARELLA to create forged prescriptions for oxycodone in their name so that they could fill those prescriptions on FARELLA's behalf. The CW advised agents, in sum and substance, that FARELLA would call various individuals on their cellphones when he had a prescription ready for them to fill at the pharmacy. The CW advised that FARELLA would often call those he recruited to arrange to pick them up and drive them to the pharmacies. Once the prescription was filled, the individuals would give the oxycodone pills to FARELLA in exchange for money.

8. Pursuant to the execution of the search warrant at the Lyghthouse Inn on March 2, 2012, agents recovered DEVICE 1 AND DEVICE 2 from inside of Room 132. Room 132 also contained two computers, a printer, blank prescriptions, prescriptions and prescriptions receipts under various names, empty oxycodone prescription bottles, identification cards in various names, a grinder containing residue, documents with the name "Frank Vincent" and other items. Agents observed PECORINO inside of Room 132 and subsequently placed her under arrest.

9. DEVICE 3 was recovered inside of Room 208 from VINCENT at the time of his arrest on March 2, 2012. Agents also recovered oxycodone prescriptions in VINCENT's name from Room 208, which prescriptions were later confirmed to be fraudulent.

10. DEVICE 4 was recovered from CABRERA at the time of his arrest on March 2, 2012 on a street in Brooklyn, New York. Agents also recovered a quantity of crack cocaine and oxycodone from CABRERA at the time of his arrest.

11. In my experience, individuals who are involved in the trafficking of narcotics typically use cellular telephones to communicate with co-conspirators about their illegal activities and to store contact information and other records related to their illegal activities. Based on my knowledge, training, and experience, I know that the SUBJECT DEVICES can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the Device. This information can sometimes be recovered with forensics tools.

IV. TECHNICAL BACKGROUND

12. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how electronic devices were used, the purpose of their use, who used

them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT DEVICES because:

a. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use. Electronic devices can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search

warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic device at a relevant time.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

13. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

14. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto the SUBJECT DEVICES. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

V. CONCLUSION

15. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the SUBJECT DEVICES there exists evidence of crimes. Accordingly, a search warrant is requested.

16. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations, and that not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly through online forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE SUBJECT DEVICES.

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court.

JOSEPH BARBATO
INVESTIGATOR
DRUG ENFORCEMENT ADMINISTRATION

Sworn
18th

THE HC
UNITEL
EASTER

J.D. GO

ATTACHMENT A

Property to Be Searched

The property to be searched is a SAMSUNG METRO PCS CELLULAR TELEPHONE, BEARING HEX NUMBER A000002A8F0298 ("DEVICE 1"); a SAMSUNG AT&T CELLULAR TELEPHONE, BEARING SERIAL NUMBER RQ6BC00349T ("DEVICE 2"); a SAMSUNG BOOST MOBILE CELLULAR TELEPHONE, BEARING HEX NUMBER A000002A7A0CC6 ("DEVICE 3"); a LG VERIZON CELLULAR TELEPHONE, BEARING SERIAL NUMBER 108CYKJ0054941 ("DEVICE 4") (collectively, the "SUBJECT DEVICES"). This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All information obtained from the SUBJECT DEVICES will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes fruits, evidence and instrumentalities of a conspiracy to distribute and possess with the intent to distribute narcotics, in violation of Title 21, United States Code, Sections 841 and 846, including:

1. All records and information on the SUBJECT DEVICES described in Attachment A, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of a conspiracy to distribute and possess with the intent to distribute narcotics, in violation of Title 21, United States Code, Sections 841 and 846;

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;

7. Evidence of the times the Device was used;

8. Passwords, encryption keys, and other access devices that may be necessary to access the Device; and

9. Contextual information necessary to understand the evidence described in this attachment,

all of which constitute evidence, fruits and instrumentalities of a conspiracy to distribute and possess with the intent to distribute narcotics, in violation of Title 21, United States Code, Sections 841 and 846.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.